***Б. Забітовський**, студент бакалаврату*
***О Харжевська**, к. пс. н., доц.*
Хмельницький національний університет

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА ЗЛОЧИНИ, ВЧИНЕНІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ (DEEPFAKE, АВТОНОМНІ СИСТЕМИ): ПРОГАЛИНИ В КК УКРАЇНИ

Стрімкий розвиток технологій штучного інтелекту (ШІ) у другому десятилітті XXI ст. породив принципово нові форми суспільно небезпечної поведінки, які чинне кримінальне законодавство України фактично не охоплює. Серед найбільш проблемних явищ виокремлюються дві групи технологій: системи генерації синтетичного медіаконтенту (deepfake) та автономні системи ШІ, здатні приймати рішення без безпосереднього людського втручання. Обидві групи технологій вже активно застосовуються для вчинення злочинів, тоді як Кримінальний кодекс України (КК України) не містить спеціальних норм, що адекватно відображали б їх суспільну небезпеку.

Аналіз актуальних наукових досліджень свідчить про зростаючий науковий інтерес до цієї проблематики. Зокрема, А. В. Піддубна та К. О. Божук досліджують виклики ШІ для кримінального провадження [1, с. 36-37], А. Семенюк-Прибатень аналізує загальні проблеми взаємодії ШІ та кримінального права [3, с. 45-46], а К. В. Юртаєва здійснює кримінологічний аналіз deepfake-технологій як нового виду злочинності [4, с. 31-33]. Попри це, комплексного дослідження прогалин КК України у цій сфері досі не проведено.

Deepfake − це аудіовізуальний або текстовий контент, синтезований або модифікований за допомогою технологій глибокого навчання (нейромереж) з метою правдоподібного відтворення зовнішності, голосу або поведінки конкретної особи. В Україні відсутнє визначення цього поняття в будь-якому нормативно-правовому акті, що саме по собі є суттєвою правовою прогалиною [4, с. 31-32; 5].

Наразі deepfake-контент застосовується для вчинення: шахрайства такі як: обходу біометричної верифікації в банківських системах, імітації особи для укладення правочинів; розповсюдження порнографічних матеріалів без згоди особи; дифамації та шантажу; поширення дезінформації з метою маніпулювання громадською думкою та дестабілізації суспільно-політичної обстановки; кібербулінгу та переслідування [4, с. 38-39].

Чинна редакція КК України кваліфікує такі дії переважно за загальними статтями: ст. 190 (шахрайство), ст. 301 (виготовлення і розповсюдження порнографічних матеріалів), ст. 182 (порушення недоторканності приватного життя). При цьому deepfake розглядається лише як «засіб» вчинення злочину, але не як самостійний предмет кримінально-правової охорони [5].

Така конструкція породжує принаймні три кваліфікаційні проблеми. По-перше, при відсутності майнової шкоди кваліфікація за ст. 190 КК України унеможливлюється через відсутність ознаки заволодіння майном. По-друге, санкції загальних статей не відображають підвищену суспільну небезпеку систематичного або масового поширення синтетичного контенту [4, с. 35-37].

По-третє, відсутні кваліфікуючі ознаки для поширення deepfake в умовах воєнного стану або з метою впливу на вибори.

Як слушно зазначає К. В. Юртаєва, чинне законодавство розглядає deepfake лише як засіб вчинення злочину, ігноруючи самостійну суспільну небезпеку створення та розповсюдження біометричних фальсифікацій [4, с. 38]. Це підтверджується і в петиції до Кабінету Міністрів України № 41/009114-26еп, яка наголошує на необхідності спеціальної кримінально-правової норми [5].

Сучасні автономні системи з ШІ, зокрема безпілотні транспортні засоби, алгоритмічні торгові платформи, системи кіберзахисту та ударні дрони, здатні самостійно виконувати дії, які містять ознаки кримінальних правопорушень, такі як спричинення смерті або тілесних ушкоджень, втручання в критичну інформаційну інфраструктуру чи заподіяння значної матеріальної шкоди [7, с. 152].

Ключова правова проблема полягає в тому, що згідно зі ст. 18 КК України суб'єктом злочину може бути лише фізична осудна особа. Автономна система, навіть така, що функціонує без прямого управління людиною, не є суб'єктом права і не може нести кримінальну відповідальність. Відповідно, відповідальність покладається на розробника алгоритму, власника або оператора системи [3, с. 47-48].

В умовах воєнного часу ця проблема набуває особливого виміру: застосування автономних ударних дронів із функціями ШІ для самостійного вибору цілей порушує питання відповідальності за порушення норм міжнародного гуманітарного права, яке чинний КК України не регулює в контексті ШІ-систем. Сучасна доктрина одностайно констатує відсутність спеціального кримінально-правового регулювання автономних систем в Україні [1; 2; 3].

Аналіз викладеного дозволяє виокремити такі системні прогалини в КК України у сфері злочинів з використанням ШІ.

1) Відсутність спеціальних складів злочинів. КК України не містить норм, які б прямо передбачали відповідальність за незаконне створення та розповсюдження deepfake-контенту або за використання автономних систем ШІ для вчинення злочинів [3, с. 49-50]. Для порівняння: EU AI Act (Регламент ЄС 2024/1689) запроваджує категорії «неприйнятного ризику» та «високого ризику» для систем ШІ, що може слугувати орієнтиром для кримінально-правового регулювання [6].

2) Відсутність легальних дефініцій. КК України не містить визначень понять «deepfake», «автономна система штучного інтелекту», «синтетичний контент», що ускладнює судово-експертну кваліфікацію та призводить до неоднакового застосування норм на практиці [4, с. 31-32; 5].

3) Процесуальні прогалини. Результати роботи систем ШІ (розпізнавання облич, виявлення deepfake, прогнозування поведінки) не мають чіткого процесуального статусу в КПК України, що унеможливлює їх використання як належних доказів без внесення змін до ст. 84, 99-101 КПК України [1, с. 39-40; 2, с. 86-88].

4) Недостатня диференціація санкцій. Кваліфікація deepfake-злочинів за загальними статтями не дозволяє врахувати масштаб поширення контенту, вплив на виборчі процеси, використання в умовах воєнного стану як кваліфікуючі ознаки, що знижує ефективність кримінально-правового впливу [4, с. 37-38].

5) Відсутність механізму відповідальності юридичних осіб. КК України не передбачає системи кримінальної відповідальності корпорацій за злочини, вчинені через їхні ШІ-системи, на відміну від законодавства більшості країн ЄС.

Отже, після проведення аналізу засвідчуємо, що КК України наразі не відповідає викликам, які породжують технології deepfake та автономних систем ШІ. Виявлені прогалини мають системний характер і охоплюють як матеріально-правовий (відсутність спеціальних складів злочинів, легальних дефініцій, диференційованих санкцій), так і процесуально-правовий аспекти (відсутність статусу ШІ-доказів у КПК України). Ефективна протидія ШІ-злочинності потребує комплексного оновлення кримінального законодавства із урахуванням міжнародного досвіду, насамперед стандартів ЄС. Терміновість таких змін зумовлена як стрімким поширенням відповідних технологій, так і воєнним контекстом, в якому deepfake та автономні системи вже активно застосовуються проти України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Піддубна А. В., Божук К. О. Штучний інтелект у кримінальному провадженні: сучасні виклики та правові перспективи // Аналітично-порівняльне правознавство. 2025. № 5. С. 36–40.
2. Удовенко Ж. В., Галаган В. І., Шкелебей В. А. Використання штучного інтелекту у кримінальному провадженні під час дії воєнного стану. *Law and Safety*. 2025. Т. 98, № 3. С. 78–90. URL: https://doi.org/10.32631/pb.2025.3.07.
3. Семенюк-Прибатень, А. (2025). ШТУЧНИЙ ІНТЕЛЕКТ І КРИМІНАЛЬНЕ ПРАВО: ВИКЛИКИ ТА ПЕРСПЕКТИВИ. Collection of Scientific Papers «SCIENTIA», (October 31, 2025; The Hague, Netherlands), 57–58. Retrieved from https://previous.scientia.report/index.php/archive/article/view/3141
4. Юртаєва К. В. Кримінологічний аналіз використання технології Deepfake: коли фейк стає злочином // Вісник Кримінологічної асоціації України. 2021. № 1(24). С. 31–39.
5. Петиція № 41/009114-26еп «Запровадження кримінальної та цивільно-правової відповідальності за несанкціоноване створення та розповсюдження шкідливого синтетичного (deepfake) контенту» від 16 січня 2026 р. URL: https://petition.kmu.gov.ua/petitions/9114
6. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. L 1689, 12.07.2024.
7. Ігнатуша В. В. Автономні системи з ШІ у збройних конфліктах та правове забезпечення дотримання принципу розрізнення // Науковий вісник Ужгородського національного університету. Серія ПРАВО. 2025. Вип. 90: частина 5. С. 151–159. URL: https://doi.org/10.24144/2307-3322.2025.90.5.18